UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P O Box 1450
Alexandria, Virginia 22313-1450
www uspto gov

| APPLICATION NO. | FILING DATE | FIRST NAMED INVENTOR | ATTORNEY DOCKET NO. | CONFIRMATION NO. |
|---|---|---|---|---|
| 10/519,586 | 12/22/2004 | Gerardus T. M. Hubert | NL02 0587 US | 9569 |

65913 7590 08/29/2008

NXP, B.V.
NXP INTELLECTUAL PROPERTY DEPARTMENT
M/S41-SJ
1109 MCKAY DRIVE
SAN JOSE, CA 95131

| EXAMINER | |
|---|---|
| SU, SARAH | |
| **ART UNIT** | **PAPER NUMBER** |
| 2131 | |

| NOTIFICATION DATE | DELIVERY MODE |
|---|---|
| 08/29/2008 | ELECTRONIC |

**Please find below and/or attached an Office communication concerning this application or proceeding.**

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

ip.department.us@nxp.com

|  |  |  |  |
|---|---|---|---|
| *Office Action Summary* | **Application No.** | **Applicant(s)** |  |
|  | 10/519,586 | HUBERT, GERARDUS T. M. |  |
|  | **Examiner** | **Art Unit** |  |
|  | Sarah Su | 2131 |  |

***-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --***

**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

1)☒ Responsive to communication(s) filed on *13 June 2008*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

4)☒ Claim(s) *1-48* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-48* is/are rejected.

7)☒ Claim(s) *1,2,11,14,15,24,25,34,37,44,46 and 47* is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

**Application Papers**

9)☒ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *22 December 2004* is/are: a)☐ accepted or b)☒ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☒ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

1) ☒ Notice of References Cited (PTO-892)

2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☒ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date *12/22/04*.

4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) ☐ Notice of Informal Patent Application

6) ☐ Other: _____.

## DETAILED ACTION

1. Preliminary Amendment A, received on 22 December 2004, and Preliminary Amendment B, received on 13 June 2008, have been entered into record. In these amendments, claims 11, 16-17, 34, 37, 39-40, 44, and 46 have been amended, and claims 49-54 have been cancelled.

2. Claims 1-48 are presented for examination.

### *Election/Restrictions*

3. Applicant's election without traverse of Group 1, Claims 1-48 in the reply filed on 13 June 2008 is acknowledged.

### *Specification*

4. The abstract of the disclosure is objected to because in line 15, "[Fig 3.]" should be removed. Correction is required. See MPEP § 608.01(b).

5. The following guidelines illustrate the preferred layout for the specification of a utility application. These guidelines are suggested for the applicant's use.

### Arrangement of the Specification

As provided in 37 CFR 1.77(b), the specification of a utility application should include the following sections in order. Each of the lettered items should appear in upper case, without underlining or bold type, as a section heading.

(a) TITLE OF THE INVENTION.
(b) CROSS-REFERENCE TO RELATED APPLICATIONS.
(f) BACKGROUND OF THE INVENTION.
(1) Field of the Invention.

(2) Description of Related Art including information disclosed under 37 CFR 1.97 and 1.98.

(g) BRIEF SUMMARY OF THE INVENTION.
(h) BRIEF DESCRIPTION OF THE SEVERAL VIEWS OF THE DRAWING(S).
(i) DETAILED DESCRIPTION OF THE INVENTION.
(j) CLAIM OR CLAIMS (commencing on a separate sheet).
(k) ABSTRACT OF THE DISCLOSURE (commencing on a separate sheet).

6. The disclosure is objected to because of the following informalities:

a. In page 4, line 20: “key 26👁” is unclear;

b. In page 19, line 1: “input effects” should read –input affects–.

Appropriate correction is required.

## ***Claim Objections***

7. The claims are objected to because the lines are crowded too closely together, making reading difficult. Substitute claims with lines one and one-half or double spaced on good quality paper are required. See 37 CFR 1.52(b).

8. Claim 46 is objected to under 37 CFR 1.75(c), as being of improper dependent form for failing to further limit the subject matter of a previous claim. Applicant is required to cancel the claim(s), or amend the claim(s) to place the claim(s) in proper dependent form, or rewrite the claim(s) in independent form. Claim 46 recites a smart card with the key generator of claim 24, which does not properly further limit claim 24.

9. Claim 14 is objected to under 37 CFR 1.75(c) as being in improper form because a multiple dependent claim should refer to other claims in the alternative only. Claim 15 is objected to under 37 CFR 1.75(c) as being in improper form because a multiple

dependent claim cannot depend from any other multiple dependent claim. See MPEP § 608.01(n). Accordingly, the claims 14-15 not been further treated on the merits.

10. Claims 1, 2, 11, 24-25, 34, 37, 44 and 47 are objected to because of the following informalities:

a. In claim 1, line 4: “the Nk words” lacks antecedent basis;

b. In claim 2, line 2: “previously generated words” is unclear if it relates to “previously generated words” (claim 1, line 14);

c. In claim 2, lines 3-4: “a respective subsequent word” is unclear if it relates to “subsequent words” (claim 1, line 13);

d. In claim 11, line 1: “method of any one of claims 1” should read –method of claim 1–;

e. In claim 24, line 4: “the Nk words” lacks antecedent basis;

f. In claim 25, line 2: “previously generated words” is unclear if it relates to "previously generated words" (claim 24, line 12);

g. In claim 34, line 1: “apparatus of any one of claim 24” should read – apparatus of claim 24–;

h. In claim 37, lines 1-2: “apparatus of any ---- preceding 24” should read – apparatus of claim 24–;

i. In claim 44, line 1: “apparatus of claim 1” should read –apparatus of claim 24–.

j. Claim 47 does not contain a proper transitional phrase. See MPEP § 2111.03.

Appropriate correction is required.

### *Drawings*

11. The drawings are objected to as failing to comply with 37 CFR 1.84(p)(5) because they include the following reference character(s) not mentioned in the description: 25 (Figure 1); 61 (Figure 2);157 (Figures 4, 5); 125 (Figure 5).

12. The drawings are objected to because: in Figure 3, "EXPENSION PROCESSOR" should read –EXPANSION PROCESSOR–.

13. The examiner notes that Figure 5 has not been specifically described in the detailed description of the specification.

Corrected drawing sheets in compliance with 37 CFR 1.121(d) are required in reply to the Office action to avoid abandonment of the application. Any amended replacement drawing sheet should include all of the figures appearing on the immediate prior version of the sheet, even if only one figure is being amended. The figure or figure number of an amended drawing should not be labeled as “amended.” If a drawing figure is to be canceled, the appropriate figure must be removed from the replacement sheet, and where necessary, the remaining figures must be renumbered and appropriate changes made to the brief description of the several views of the drawings for consistency. Additional replacement sheets may be necessary to show the renumbering of the remaining figures. Each drawing sheet submitted after the filing date of an application must be labeled in the top margin as either “Replacement Sheet” or “New Sheet” pursuant to 37 CFR 1.121(d). If the changes are not accepted by the examiner, the applicant will be notified and informed of any required corrective action in the next Office action. The objection to the drawings will not be held in abeyance.

### ***Claim Rejections - 35 USC § 112***

14. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

15. Claims 1 and 24 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. Claim 1 recites the limitation "the Nk words" in line 4 and claim 24 recites the limitation “the Nk words” in line 4. There is insufficient antecedent basis for these limitations in the claims.

### ***Claim Rejections - 35 USC § 102***

16. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

17. Claims 1-4, 6-7, 13, 20, 22-27, 29-30, 36-37, and 43-47 are rejected under 35 U.S.C. 102(b) as being anticipated by Daemen et al. (AES Proposal: Rijndael and Daemen hereinafter).

As to claims 1 and 24, Daemen discloses a method for a Rijndael cipher and inverse cipher in block encryption/decryption, the method having:

> **storing the Nk words of the initial key in Nk locations of a memory** (page 14, line 33);
>
> **providing the initial key to a cryptographic engine for performing a first cryptographic round** (page 14, lines 33-34);
>
> **repeatedly retrieving a selected first word and a selected second word of the expanded key, at least one of which is retrieved from the memory, and generating from the selected first and second words a successive subsequent word of the expanded key** (page 14, lines 33-34);
>
> **providing the generated words of the expanded key to the cryptographic engine as round keys for performing subsequent cryptographic rounds** (page 14, lines 9-11);
>
> **storing successive ones of the generated subsequent words in the memory by cyclically overwriting previously generated words of the expanded key** (page 15, lines 26-28; page 17, lines 10-11).

As to claims 2 and 25, Daemen discloses:

> **in which the step of overwriting previously generated words only occurs after those words have been used as said first and/or said second selected words in the step of generating a respective subsequent word** (page 19, lines 1-2).

As to claims 3 and 26, Daemen discloses:

**in which the number of memory locations used is less than the number of words in the expanded key** (page 14, line 33).

As to claims 4 and 27, Daemen discloses:

**in which the number of memory locations used is equal to Nk** (page 14, line 33).

As to claims 6 and 29, Daemen discloses:

**in which the number of memory locations used is equal to 2Nk** (page 14, line 33; page 15, lines 26-28).

As to claims 7 and 30, Daemen discloses:

**in which the memory is divided into two parts, a first part storing the initial key and the second part receiving the successively generated words of the expanded key** (page 14, lines 20-26).

As to claims 13 and 36, Daemen discloses:

**in which the number of memory locations used is equal to 2Nk, the first and the second parts having Nk locations each** (page 14, line 33; page 15, lines 26-28).

As to claims 20 and 43, Daemen discloses:

**in which, in the retrieving step, the selected first word is retrieved from memory** (i.e. W[i-$N_k$], key) **and the selected second word is retrieved from a register used in a previous iteration** (i.e. W[i-1]) (page 14, lines 23-26).

As to claims 22 and 44, Daemen discloses:

**in which the step of generating includes, in at least some cycles of round key word generation, the step of performing an S-box transform using an S-box shared with the cryptographic engine** (page 17, lines 17-18; page 18, line 18).

As to claims 23 and 45, Daemen discloses:

**the step of maintaining synchronism** (i.e. parallel) **of the generation of successive round key words with consumption of the round key words by the cryptographic engine** (page 18, lines 21-25; page 19, lines 4-5).

As to claim 37, Daemen discloses:

**in which the expansion processor includes means for generating successive words of the AES Rijndael block cipher round keys according to the AES key expansion function** (page 8, lines 30-31).

As to claim 46, Daemen discloses:

**a smart card incorporating the round key generator according to claim 24** (page 16, lines 25-26).

As to claim 47, Daemen discloses:

**generating successive round key words of an expanded key, from an initial key** (page 14, lines 33-34)**, which method maintains the generated successive round key words in memory substantially only as long as they are required for use in the generation of successive round key words** (page 19, lines 1-2) **and for use in the parallel operation of a cryptographic process** (page 18, lines 21-25; page 19, lines 4-5).

## *Claim Rejections - 35 USC § 103*

18. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

19. Claims 5, 11-12, 18-19, 21, 28, 34-35, 41-42 are rejected under 35 U.S.C. 103(a) as being unpatentable over Daemen as applied to claims 1 and 24 above, and in view of Snell (US 2003/0223580 A1).

As to claims 5 and 28, Daemen does not disclose:

> **in which the words of the initial key are also overwritten by words of the expanded key during the overwriting step.**

Nonetheless, this feature is well known in the art and would have been an obvious modification of the teachings disclosed by Daemen, as evidenced by Snell.

Snell discloses a system and method for advanced encryption standard hardware cryptographic engine, the system and method having:

> **in which the words of the initial key are also overwritten by words of the expanded key during the overwriting step** (0082, lines 3-7), where an encryption process is followed by a decryption process.

Given the teaching of Snell, a person having ordinary skill in the art at the time of the invention would have readily recognized the desirability and advantages of modifying the teachings of Daemen with the teachings of Snell by overwriting the initial key. Snell recites motivation by disclosing that the cipher keys are needed for key expansion (0008, lines 1-2) and that decryption can be done by inverting the cipher transformations and performing the key schedule in reverse order (0009, lines 1-5). Therefore, data can be encrypted or decrypted starting with the cipher key in a certain location in order to reduce memory requirements (0011, lines 2-7). It is obvious that the teachings of Snell would have improved the teachings of Daemen by overwriting an initial key in order to reduce memory requirements by storing keys needed for encryption and decryption in a single location.

As to claims 11 and 34, Daemen does not disclose:

> **the step of completing generation of the expanded key such that the final round key is stored in the memory and the initial key has been overwritten.**

Nonetheless, this feature is well known in the art and would have been an obvious modification of the teachings disclosed by Daemen, as evidenced by Snell.

Snell discloses:

> **the step of completing generation of the expanded key such that the final round key is stored in the memory and the initial key has been overwritten** (0082, lines 3-7).

Given the teaching of Snell, a person having ordinary skill in the art at the time of the invention would have readily recognized the desirability and advantages of modifying the teachings of Daemen with the teachings of Snell by overwriting the initial key with the final key. Please refer to the motivation disclosed above in respect to claims 5 and 28 as to why it is obvious to apply the teachings of Snell to the teachings of Daemen.

As to claims 12 and 35, Daemen discloses:

> **the step of performing an inverse key expansion starting with the final round key stored in the memory in order to regenerate the initial key for a subsequent cryptographic operation** (page 22, lines 9-10).

As to claims 18 and 41, Daemen does not disclose:

> **in which the step of providing the generated words of the expanded key to the cryptographic engine comprises providing the words on a word-by-word basis as the cryptographic engine consumes the words as round keys.**

Nonetheless, this feature is well known in the art and would have been an obvious modification of the teachings disclosed by Daemen, as evidenced by Snell.

Snell discloses:

> **in which the step of providing the generated words of the expanded key to the cryptographic engine comprises providing the words on a word-by-word basis as the cryptographic engine consumes the words as round keys** (0082, lines 2-10).

Given the teaching of Snell, a person having ordinary skill in the art at the time of the invention would have readily recognized the desirability and advantages of modifying the teachings of Daemen with the teachings of Snell by providing words word-by-word to a cryptographic engine. Snell recites motivation by disclosing that the transformation sequence in the reverse direction must be the same as that applied in the forward key expansion (0081, lines 17-19). It is obvious that the teachings of Snell would have improved the teachings of Daemen by providing words word-by-word in order to ensure that the proper order is executed.

As to claims 19 and 42, Daemen does not disclose:

> **in which, in the retrieving step, both the selected first word and the selected second word are retrieved from the memory.**

Nonetheless, this feature is well known in the art and would have been an obvious modification of the teachings disclosed by Daemen, as evidenced by Snell.

Snell discloses:

> **in which, in the retrieving step, both the selected first word and the selected second word are retrieved from the memory** (0010, lines 2-4).

Given the teaching of Snell, a person having ordinary skill in the art at the time of the invention would have readily recognized the desirability and advantages of modifying the teachings of Daemen with the teachings of Snell by retrieving words from memory. Snell recites motivation by disclosing that storing data in memory allows for faster subsequent execution of cryptographic rounds (0010, lines 6-7). It is obvious that the teachings of Snell would have improved the teachings of Daemen by retrieving data from memory in order to provide for faster execution.

As to claim 21, Daemen does not disclose:

> **in which the step of providing the generated words of the expanded key to the cryptographic engine comprises providing said generated words from the memory.**

Nonetheless, this feature is well known in the art and would have been an obvious modification of the teachings disclosed by Daemen, as evidenced by Snell.

Snell discloses:

> **in which the step of providing the generated words of the expanded key to the cryptographic engine comprises providing said generated words from the memory** (0010, lines 2-4)**.**

Given the teaching of Snell, a person having ordinary skill in the art at the time of the invention would have readily recognized the desirability and advantages of modifying the teachings of Daemen with the teachings of Snell by providing words from memory. Please refer to the motivation recited above in respect to claims 19 and 42 as to why it is obvious to apply the teachings of Snell to the teachings of Daemen.

20. Claims 8-10, 16-17, 31-33, 38-40, and 48 are rejected under 35 U.S.C. 103(a) as being unpatentable over Daemen as applied to claims 1, 24, and 47 above, and in view of Yup et al. (US 2002/0191784 A1 and Yup hereinafter).

As to claims 8 and 31, Daemen does not disclose:

**the step of completing generation of the expanded key such that the final round key is stored in the second part of the memory and the initial key is still stored in the first part of the memory.**

Nonetheless, this feature is well known in the art and would have been an obvious modification of the teachings disclosed by Daemen, as evidenced by Yup.

Yup discloses a system and method for implementing the advanced encryption standard block cipher algorithm in a system with a plurality of channels, the system and method having:

**the step of completing generation of the expanded key such that the final round key is stored in the second part of the memory** (0019, lines 5-9) **and the initial key is still stored in the first part of the memory** (0028, lines 3-5)**.**

Given the teaching of Yup, a person having ordinary skill in the art at the time of the invention would have readily recognized the desirability and advantages of modifying the teachings of Daemen with the teachings of Yup by storing an initial key and a final key. Yup recites motivation by disclosing that an encryption/decryption means can selectively encrypt or decrypt data based on a control signal (0017, lines 22-26). It is obvious that the teachings of Yup would have improved the teachings of Daemen by storing an initial and final key so that encryption or decryption can be performed based on a signal.

As to claims 9 and 32, Daemen discloses:

**the step of performing a repeat key expansion starting with the initial key stored in the first part of the memory** (page 14, lines 33-34).

As to claims 10 and 33, Daemen does not disclose:

**the step of performing an inverse key expansion starting with the final round key stored in the second part of the memory.**

Nonetheless, this feature is well known in the art and would have been an obvious modification of the teachings disclosed by Daemen, as evidenced by Yup.

Yup discloses:

**the step of performing an inverse key expansion starting with the final round key stored in the second part of the memory** (0019, lines 5-9).

Given the teaching of Yup, a person having ordinary skill in the art at the time of the invention would have readily recognized the desirability and advantages of modifying the teachings of Daemen with the teachings of Yup by performing key expansion with the final key. Yup recites motivation by disclosing that storing a final key and using it for decryption does not require for the entire key expansion to be performed to get the last key, saving processing and set-up time for decryption operations (0042, lines 6-9). It is obvious that the teachings of Yup would have improved the teachings of Daemen by starting with a stored final key for inverse key expansion in order to save processing and set-up time for decryption.

As to claims 16 and 39, Daemen does not disclose:

**in which the successive subsequent words of the expanded key comprise words of encryption round keys.**

Nonetheless, this feature is well known in the art and would have been an obvious modification of the teachings disclosed by Daemen, as evidenced by Yup.

Yup discloses:

**in which the successive subsequent words of the expanded key comprise words of encryption round keys** (0017, lines 12-20).

Given the teaching of Yup, a person having ordinary skill in the art at the time of the invention would have readily recognized the desirability and advantages of modifying the teachings of Daemen with the teachings of Yup by using the expanded key as encryption round keys. Please refer to the motivation recited above in respect to claims 8 and 31 as to why it obvious to apply the teachings of Yup to the teachings of Daemen.

As to claims 17 and 40, Daemen does not disclose:

**in which the successive subsequent words of the expanded key comprise words of decryption round keys.**

Nonetheless, this feature is well known in the art and would have been an obvious modification of the teachings disclosed by Daemen, as evidenced by Yup.

Yup discloses:

**in which the successive subsequent words of the expanded key comprise words of decryption round keys** (0019, lines 7-9).

Given the teaching of Yup, a person having ordinary skill in the art at the time of the invention would have readily recognized the desirability and advantages of modifying the teachings of Daemen with the teachings of Yup by using the expanded key as decryption round keys. Please refer to the motivation recited above in respect to claims 8 and 31 as to why it obvious to apply the teachings of Yup to the teachings of Daemen.

As to claim 38, Daemen does not disclose:

**in which Nk=8.**

Nonetheless, this feature is well known in the art and would have been an obvious modification of the teachings disclosed by Daemen, as evidenced by Yup.

Yup discloses:

**in which Nk=8** (0036, lines 1-2**).**

Given the teaching of Yup, a person having ordinary skill in the art at the time of the invention would have readily recognized the desirability and advantages of modifying the teachings of Daemen with the teachings of Yup by using a key size of 8. Yup recites motivation by disclosing that having a key size of 8 requires modification to the key generation algorithm (0037, lines 1-2) because of the key size. It is obvious that the teachings of Yup would have improved the teachings of Daemen by using a key size of 8 in order to accommodate larger key sizes by modifying the key generation algorithm.

As to claim 48, Daemen does not disclose:

**in which the initial key words are also maintained in the memory during the entire process of generating the expanded key**.

Nonetheless, this feature is well known in the art and would have been an obvious modification of the teachings disclosed by Daemen, as evidenced by Yup.

Yup discloses:

**in which the initial key words are also maintained in the memory during the entire process of generating the expanded key** (0028, lines 3-5).

Given the teaching of Yup, a person having ordinary skill in the art at the time of the invention would have readily recognized the desirability and advantages of modifying the teachings of Daemen with the teachings of Yup by keeping an initial key. Please refer to the motivation recited above in respect to claims 8 and 31 as to why it obvious to apply the teachings of Yup to the teachings of Daemen.

## ***Conclusion***

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Sarah Su whose telephone number is (571) 270-3835. The examiner can normally be reached on Monday through Friday 7:30AM-5:00PM EST..

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on (571) 272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Sarah Su/
Examiner, Art Unit 2131
/Ayaz R. Sheikh/
Supervisory Patent Examiner, Art Unit 2131